

**Annual 47 C.F.R. § 64.2009(e) CPNI Certification**

**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2008

Date filed: February 27, 2009

Name of company(s) covered by this certification: E.Com Technologies, LLC dba FirstMile Technologies

Form 499 Filer ID: **820556**

Name of signatory: Michael E. Keller

Title of signatory: Chief Financial Officer


I, Michael E. Keller, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See 47 C.F.R. § 64.2001 et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed



### **CPNI Usage Policy Statement**

Pursuant to Section 64.2009(e) of the Federal Communications Commission's rules, this statement explains how E-Com Technologies, LLC's dba FirstMile and dba FirstMile Technologies (Company) operating procedures ensure compliance with Part 64, Subpart U, of the FCC's rules.

#### **Company's Usage of CPNI**

The Company has CPNI Procedures that set forth the Company's CPNI policies and outline what CPNI is and when it may or may not be used without customer approval by the Company.

The Company does not currently use CPNI for marketing purposes. Should the Company ever decide to expand their marketing efforts and use CPNI for marketing purposes, the Company will comply with all FCC CPNI requirements including all Notice and approval procedures.

The Company's Procedures set forth that the use of CPNI for the purpose of marketing a service to which a customer does not already subscribe is prohibited without prior customer notice and approval. The Company will not provide to any affiliate, CPNI of any customer who does not also subscribe to the services provided by that affiliate, without prior customer notice and approval.

The Company's Procedures clearly set forth when CPNI may be used without customer approval. The Company's Procedures provide that the Company may use CPNI to protect its rights and property, customers, and other carriers from fraudulent, abusive or unlawful use of, or subscription to, Company's services.

The Company's Procedures require affirmative written/electronic customer approval for the release of CPNI to third parties.

#### **Company's CPNI Safeguards**

The Company has established procedures for the training of its personnel. Employees have been trained as to when they are and are not authorized to use CPNI. The Company's CPNI Procedures describe the disciplinary process related to noncompliance with CPNI obligations, which can include termination of employment.

The Company has established a supervisory review process regarding Company compliance with the FCC's CPNI rules. The Company's supervisory process ensures compliance with the FCC's rules on outbound marketing situations, and the Company maintains records of compliance with these rules. The Company's procedures require that all sales personnel obtain supervisory approval of any proposed outbound marketing request.

The Company has appointed a corporate officer that has been named as the CPNI Compliance Officer and is held responsible for annually certifying that the Company is in compliance with the FCC's CPNI rules and submitting such certification and accompanying statement of how the company complies with the FCC's CPNI rules to the FCC by March 1.

The Company takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Company authenticates a customer prior to disclosing CPNI based on customer initiated telephone contact, online account access, or an in-store visit.

The Company only discloses call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides a password that is not prompted by the carrier asking for readily available biographical information or account information. If a customer does not provide a password, Company only discloses call detail information by sending it to an address of record or by calling the customer at the telephone of record. If the customer is able to provide call detail information during a customer-initiated call without Company's assistance, then Company is permitted to discuss the call detail information provided by the customer.

The Company has established a system of passwords and password protection. For a new customer, Company requests that the customer establish a password at the time of service initiation. For existing customers to establish a password, Company must first authenticate the customer without the use of readily available biographical information or account information. Company authenticates a customer using non-public information such as calling the customer at the telephone number of record or using a Personal Identification Number (PIN) method to authenticate a customer.

For accounts that are password protected, Company cannot obtain the password by asking for readily available biographical information or account information to prompt the customer for his password. A customer may also access call detail information by establishing an online account or by visiting a carrier's retail location. If a password is forgotten or lost, Company uses a back-up customer authentication method that is not based on readily available biographical information or account information.

If a customer does not want to establish a password, the customer may still access call detail based on a customer-initiated telephone call, by asking Company to send the call detail information to an address of record or by the carrier calling the telephone number of record.

If a customer is able to provide to the Company, during a customer-initiated telephone call, all of the call detail information necessary to address a customer service issue (i.e., the telephone number called, when it was called, and if applicable, the amount charged for the call) then Company proceeds with its routine customer carrier procedures. Under these circumstances, Company may not disclose to the customer any call detail

information about the customer account other than the call detail information that the customer provides without the customer first providing a password.

Company password-protects online access to all CPNI, call detail and non-call detail.

Company may provide customers with access to CPNI at a carrier's retail location if the customer presents a valid photo ID and the valid photo ID matches the name on the account.

Company notifies a customer immediately when a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record.

Company maintains a record of any discovered breaches and notifications to the USSS and the FBI regarding those breaches, as well as the USSS and the FBI response to the notifications for a period of at least two year.

#### **Actions Taken Against Data Brokers and Customer Complaints**

Company has taken no actions against data brokers in the past year. Company has received no customer complaints in the past year concerning the unauthorized released of CPNI.

In the event of a CPNI breach, Company complies with the FCC's rules regarding notice to law enforcement and customers. Company maintains records of any discovered breaches and notifications to the United States Secret Service (USSS) and the FBI regarding those breaches, as well as the USSS and the FBI responses to the notifications for a period of at least two year.

#### **Actions Taken Against Data Brokers and Customer Complaints**

Company has taken no actions against data brokers in the last year. Company has received no customer complaints in the past year concerning the unauthorized released of CPNI.